IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

TOMI HARTLEY, individually and on behalf of all others similarly situated, Plaintiff, v. URBAN OUTFITTERS, INC., Defendant.	CASE NO. 2:23-CV-04891-CMR

PLAINTIFF'S MEMORANDUM OF LAW IN SUPPORT OF HER RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION TO DISMISS

I. INTRODUCTION

Plaintiff Tomi Hartley ("Plaintiff") alleges that Defendant Urban Outfitters, Inc. ("Defendant" or "Urban Outfitters"), in violation of A.R.S. § 44-1376.01, invaded her privacy by unlawfully spying on the time and place she read emails from Urban Outfitters, through spy pixel tracking software placed without Plaintiff's consent. Because Plaintiff has Article III standing to bring her claim in this Court and because Plaintiff properly alleges a violation of A.R.S. § 44-1376.01, the Court should deny Defendant's Motion to Dismiss (ECF No. 10-1) ("MTD").

II. FACTS

This case involves Urban Outfitters tracking Plaintiff's email reading activity without her consent. Compl. ¶¶ 4, 9, 38. As part of its marketing practices, Urban Outfitters tracks the time and place its email recipients open their email marketing emails. *Id.* ¶¶ 4, 32-38, 48-49. Defendant tracks email reading activity in order gain "engagement data [and] directional insights into [] subscribers' behaviors." *Id.* ¶ 34. From August 2022 to November 2023, Plaintiff received

promotional emails from Urban Outfitters. *Id.* ¶ 7. Plaintiff most recently opened an email from Defendant in November 2023. *Id.* Little did Plaintiff know Defendant was tracking and recording every time she opened an email from Urban Outfitters. *Id.* ¶¶ 8-9, 52-53. Urban Outfitters tracked the time and place where Plaintiff opened the emails. *Id.* ¶¶ 8-9, 37, 52-53. This invaded Plaintiff's right to privacy. *Id.* ¶ 55. Plaintiff never consented to Defendant's tracking practices. *Id.* ¶¶ 4-5, 9, 38, 53.

Plaintiff alleges that this conduct violates A.R.S. § 44-1376.01. *Id.* ¶¶ 1, 46-56. A.R.S. § 44-1376.01 was enacted in response to the Hewlett-Packard ("HP") pretexting scandal. *Id.* ¶ 27. The HP pretexting scandal involved HP's board surreptitiously procuring the telephone and email records of newspaper reporters in an effort to catch leakers. *Id.* ¶¶ 14-26. Congress held a hearing and brought to light HP's invidious behavior. *Id.* ¶ 25. During the hearing, Congress uncovered how HP used spy tracking pixel to record when, where, and who opened the emails that were sent to the newspaper reporters. *Id.* The discovery shocked the Congressional committee. *Id.* In response Congress passed the Telephone Records Protection Act, 18 U.S.C. § 1039, and Arizona passed A.R.S. § 44-1376 *et seq*. *Id.* ¶¶ 26-27.

III. ARGUMENT

This action is properly brought to this court. First, Plaintiff has Article III standing for her claim because a violation of A.R.S. § 44-1376 is a substantive invasion of privacy—a harm traditionally recognized as providing a basis for a lawsuit in American courts. *See TransUnion LLC v. Ramirez*, 594 U.S. 413, 424 (2021). Second, Plaintiff properly alleges a violation of A.R.S. § 44-1376.01 because she alleges that Urban Outfitters "procured" her "communication service records" through a spy pixel that created an "access log" of the time and place she read her emails.

A. Plaintiff Has Article III Standing To Bring Her Claims

Defendant argues that this Court lacks subject matter jurisdiction because Plaintiff does not allege "any 'concrete' injury … as a result of this alleged invasion of privacy." MTD at 5. Defendant is wrong. Courts in this district and elsewhere have repeatedly held that violations of statutes based on the torts of invasion of privacy or intrusion upon seclusion give rise to Article III standing.

1. Legal Standard

When a defendant moves to dismiss a complaint pursuant to Rule 12(b)(1) and disputes whether the facts as pleaded create Article III standing, it is considered a facial standing challenge. *Iwaniw v. Early Warning Servs., LLC*, 2021 WL 3209856, at *1 (E.D. Pa. July 28, 2021) (Rufe, J.) (citing *Kamal v. J. Crew Grp., Inc.*, 918 F.3d 102, 109 (3d Cir. 2019)). A facial attack "is an argument that considers a claim on its face and asserts that it is insufficient to invoke the subject matter jurisdiction of the court ... ." *Id.* (quoting *Constitution Party of Pa. v. Aichele*, 757 F.3d 347, 358 (3d Cir. 2014)). In reviewing a facial standing challenge, a court may find that the complaint's general allegations of injury-in-fact are adequate if the complaint "'clearly and specifically set[s] forth facts sufficient to satisfy' Article III." *Id.* (quoting *Kamal*, 918 F.3d at 109). The court must consider the alleged facts in the light most favorable to the plaintiff. *Id.* (citing *Aichele*, 757 F.3d at 358)

2. Defendant's Invasion Of Plaintiff's Privacy Is A Concrete Harm

Constitutional standing requires three elements: "injury in fact," "a causal connection between the injury and the conduct complained of," and a likelihood that a favorable decision will redress the plaintiff's injury. *Ricks v. Medicredit, Inc.*, 2022 WL 11398285, at *2 (E.D. Pa. Oct. 18, 2022) (Rufe, J.) (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61 (1992)). "To

establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Id.* (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 339 (2016)). For an injury to be "concrete," it must be "real, and not abstract." *Id.* (quoting *TransUnion LLC v. Ramirez*, 594 U.S. 413, 424 (2021)). To determine the "concreteness" of intangible injuries, *TransUnion* instructs us to ask "whether the asserted harm has a 'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts—such as physical harm, monetary harm, or various intangible harms." *Barclift v. Keystone Credit Servs., LLC*, 93 F.4th 136, 145 (3d Cir. 2024) (quoting *TransUnion*, 594 U.S. at 417). While a plaintiff does not need to "exactly duplicate" a traditionally recognized harm, she must still analogize to a harm of the same character of previously existing legally cognizable injuries. *Id.* (citing *TransUnion*, 594 U.S. at 433, and *Kamal*, 918 F.3d at 114) (quotations omitted).

Courts in this circuit have consistently held post-*TransUnion* that a statutory violation rising in invasion of privacy is exactly the kind of harm traditionally recognized as providing a basis for a lawsuit in American courts. *See Barclift*, 93 F.4th at 145 ("At common law, actionable invasions of privacy are typically categorized into four separate torts."); *Huber v. Simon's Agency, Inc.*, 84 F.4th 132, 153 (3d Cir. 2023) ("In *TransUnion*, the cognizable harm from wrongly identifying the class members as potential terrorists was akin to the harm from defamation. In *Horizon*, the cognizable harm from the unauthorized release of the plaintiffs' sensitive information was akin to the harm from invasion of privacy, as was the disclosure of the plaintiff's financial information in *St. Pierre*, and the intrusion of an unauthorized robocall in *Susinno*.") (citations removed). The standing element of this case is no different than violations of the Video Privacy Protection Act ("VPPA"), 18 U.S.C. § 2710, and the Telephone Consumer Protection Act

("TCPA"), 47 U.S.C. § 227, where courts—post-*TransUnion*—have found that violations of the substantive privacy rights elevated by those statutes conferred Article III standing. *See Doyle v. Matrix Warranty Sols., Inc.*, 2023 WL 4188313, at *1, *1 n.2 (D.N.J. June 26, 2023) (finding allegations of receiving a prerecorded phone call in violation of TCPA to be sufficient for Article III standing and upholding *Susinno v. Work Out World, Inc.*, 862 F.3d 346 (3d Cir. 2017) in light of *TransUnion*); *Braun v. Philadelphia Inquirer, LLC*, 2023 WL 7544160, at *5 (E.D. Pa. Nov. 13, 2023) (holding that since plaintiffs established "the necessary elements for a tort claim for violation of the VPPA," plaintiffs had Article III standing); *see also Dickson v. Direct Energy, LP*, 69 F.4th 338, 343 (6th Cir. 2023) ("Here, we find that [plaintiff's] claims satisfy the demands of Article III because his alleged injury under the TCPA constitutes a concrete harm."); *Drazen v. Pinto*, 74 F.4th 1336, 1345 (11th Cir. 2023) ("[T]he harm associated with an unwanted text message shares a close relationship with the harm underlying the tort of intrusion upon seclusion. … For that reason, the harms are similar in kind, and the receipt of an unwanted text message causes a concrete injury."); *Salazar v. Nat'l Basketball Ass'n*, 2023 WL 5016968, at *6 (S.D.N.Y. Aug. 7, 2023) (finding Article III standing for VPPA violations because it is similar to intrusion upon seclusion under the Restatement (Second) of Torts § 652B (1977)). Just as substantive violations of the VPPA and TCPA—despite not being "sufficiently offensive" to satisfy common law threshold—give rise to Article III standing because they have "close relationship to harms recognized by American courts," violations of A.R.S. § 44-1376 also give rise to Article III standing.

Defendant argues that "Plaintiff has not asserted any facts showing how the recording of when she opened and read an email she requested invaded her privacy." MTD at 1. But Defendant misses the point. Arizona, where Plaintiff resides and where the violation arose, has adopted the

Restatement (Second) of Torts § 652B. *Hart v. Seven Resorts Inc.*, 190 Ariz. 272, 279 (Ct. App. 1997). A plaintiff may recover for intrusion if she "had an objectively reasonable expectation of seclusion or solitude in [a] … data source." *Med. Lab. Mgmt. Consultants v. Am. Broad. Cos.*, 30 F. Supp. 2d 1182, 1188–89 (D. Ariz. 1998) (quotation omitted). Here, Plaintiff alleges that Defendant spied on the time and place she opened emails in violation of A.R.S. § 44-1376.01. Compl. ¶¶ 33, 32-38, 46-56. And A.R.S. § 44-1376.01 was passed to elevate Arizona residents' substantive privacy rights concerning "communication service records," which includes "electronic mail." *Id.* ¶ 27; A.R.S. § 44-1376; AZ H.R. B. Summ., 2007 Reg. Sess. H.B. 2726. Similar intrusions, such as intercepting and sorting mail, *Miller v. Brooks*, 123 N.C. App. 20, 26 (1996), and obtaining phone call records, *Lawlor v. N. Am. Corp. of Illinois*, 2012 IL 112530, ¶¶ 8, 33-35, have been recognized to be actionable under the Restatement. Thus, the "harm" alleged here—invasion of privacy—"has a 'close relationship' to a harm traditionally recognized … in American courts," *Barclift*, 93 F.4th at 142, and the Arizona legislature "has used its lawmaking powers to recognize a lower quantum of injury necessary to bring a claim" under A.R.S. § 44-1376.01, *Drazen*, 74 F.4th at 1245.

Defendant cites two wiretapping cases, *Cook v. GameStop, Inc.*, 2023 WL 5529772 (W.D. Pa. Aug. 28, 2023) and *In re: BPS Direct, LLC*, 2023 WL 8458245 (E.D. Pa. Dec. 5, 2023), to support its contention that Plaintiff must allege an undefined high bar of "invasion of privacy." MTD at 5-7. But Defendant overlooks a key differentiating factor. The wiretapping statutes at issue in those cases do not identify the threshold for what data interception is considered private for a violation. *See* 18 Pa.C.S. § 5703 (prohibiting the interception of "***any*** wire, electronic or oral communication") (emphasis added). In other words, these statutes do not "elevate" the privacy interest in of a certain data *type*, the statutes just prohibit a *manner* of invasion—wiretapping. The

courts, therefore, were faced with a question: what is the minimum threshold considered private enough to give rise to Article III standing in a wiretap violation? Because the statutes are silent on this point, the courts found that interception of "any" information is too low of a threshold. *See Cook*, 2023 WL 5529772, at *3 (rejecting the assertion that "the mere fact that [defendant] recorded ***any*** information about [plaintiff]" is enough to give standing) (emphasis original); *In re BPS Direct, LLC*, 2023 WL 8458245, at *10-12 (rejecting the argument that "the conduct of the wiretapping itself, regardless of the sensitivity of the content captured" gives rise to standing). Since the wiretapping statutes do not elevate any specific private data types, the courts had to look to common law analogues to establish what is reasonably private. *Cook*, 2023 WL 5529772, at *3 ("[T]he Court must examine the nature of the information … allegedly intercepted and determine whether the interception of that kind of information amounts to an invasion of privacy interests that have been historically protected.") (citation omitted); *In re BPS Direct, LLC*, 2023 WL 8458245, at *10 (quoting *Cook*). However, requiring every statutory invasion of privacy claim to have the same standards and "elements" as a common law claim would turn *TransUnion* on its head. *See Barclift* at 145 ("*TransUnion* speaks only of harms, not elements. Indeed, the word 'element' does not appear once in the body of the *TransUnion* opinion. We believe that if the Court wanted us to compare elements, it would have simply said so."). Here, where the Arizona legislature elevated the privacy interest of a discrete data type—email records—Plaintiff is only required to allege the invasion specified by the statute just like a plaintiff in a TCPA or VPPA claim. *See In re BPS Direct, LLC*, 2023 WL 8458245, at *16 n.174 (acknowledging that substantive violations of the VPPA constitutes "concrete harm"); *Braun*, 2023 WL 7544160, at *5 (holding that VPPA allegations sufficient to overcome a Rule 12(b)(6) challenge is sufficient for Article III standing); *Doyle*, 2023 WL 4188313, at *1 ("Plaintiff in this case would meet his

standing burden by alleging receipt of a single unwanted call [in violation of the TCPA]."); *Drazen*, 74 F.4th at 1345 ("While an unwanted text message is insufficiently offensive to satisfy the common law's elements, Congress has used its lawmaking powers to recognize a lower quantum of injury necessary to bring a claim under the TCPA.").

Defendant next cites an unreported pre-*TransUnion* case, *Nyanhongo v. Credit Collection Servs.*, 2021 WL 1546233 (E.D. Pa. Apr. 20, 2021), to support its contention that Plaintiff must allege that "private, sensitive, or confidential information" was procured by Urban Outfitters. MTD at 7-8. But this case offers no support for such position, and, if anything, supports Plaintiff's position.

First, as stated above, email records of the time and place where Plaintiff opened her emails is objectionably private and confidential information. Second, *Nyanhongo* concerns a violation of the Fair Debt Collection Practices Act ("FDCPA"), 15 U.S.C. § 1692f(8), which prohibits debt collectors from using "any language or symbol" on a debt collection envelope. *Nyanhongo*, 2021 WL 1546233 at *1. Plaintiff Nyanhongo alleged that she received a debt collection envelope that had "data symbols similar to a QR code." *Id.* But Nyanhongo did not allege that scanning the QR would reveal "any personal or private information." *Id.* The court held that if the QR code would reveal an account number, there would be grounds for Article III standing. *Id.* at 3. But since Nyanhongo did not allege that the QR on her envelope was anything more than a "generic phrase that may or may not be unique to debt collection mailings," she did not plead concrete injury. *Id.* In short, Nyanhongo's failure to allege *any* sort of privacy violation doomed standing in her case. Notably, the court did not require any analogy to the common law standard of intrusion upon seclusion but rather the court found that Nyanhongo's allegation did not meet the *statutory* invasion of privacy, as opposed to other FDCPA cases where courts found standing. *Id.* at 4.

("Our Court held that a client number on the exterior of a mailer constitutes a concrete injury because it has the potential to implicate a core concern animating the FDCPA—invasion of privacy.") (cleaned up). If anything, this case shows that where a plaintiff alleges a statutory violation that implicates an invasion of privacy, there is concrete injury. And this is exactly what Plaintiff alleges here: A.R.S. § 44-1376.01 prohibits the procurement of "communication service records" which include records of the time and place where an email was read by the recipient. Compl. ¶¶ 4, 8, 32-38, 55.

In sum, A.R.S. § 44-1376.01 elevates Arizona residents' substantive privacy rights by prohibiting the procurement of "communication service records" which include "subscriber information," toll bills or "access logs," "records of the path of an electronic communication between the point of origin and the point of delivery" and "nature of the communication service provided, such as … electronic mail." A.R.S. § 44-1376.01; *see TransUnion*, 594 U.S. at 425 ("[A legislature] may elevate to the status of legally cognizable injuries concrete, de facto injuries that were previously inadequate in law.") (internal quotations omitted). Procuring communication service records in violation of the statute is an invasion of privacy and thus, Plaintiff has Article III standing to bring her claim.

B. Plaintiff Sufficiently Alleges A Claim Under A.R.S. § 44-1376.01

1. Legal Standard

Under Rule 12(b)(6), dismissal of a complaint for failure to state a claim is appropriate where a plaintiff's "plain statement" lacks enough substance to show that they are entitled to relief. *Iwaniw*, 2021 WL 3209856, at *2 (citing *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 557 (2007)). In determining whether a motion to dismiss should be granted, the court must "accept as true all allegations in the complaint and all reasonable inferences that can be drawn therefrom," and

consider them in the light most favorable to the non-moving party. *Id.* (quoting *DeBenedictis v. Merrill Lynch & Co.*, 492 F.3d 209, 215 (3d Cir. 2017)). A court is not, however, required to accept as true "a legal conclusion couched as a factual allegation." *Id.* (quoting *Twombly*). To survive a motion to dismiss, the complaint's "factual allegations must be enough to raise a right to relief above the speculative level." *Id.* (quoting *Twombly*). That is, a plaintiff must plead "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* (quoting *Gelman v. State Farm Mut. Ins. Co.*, 583 F.3d 187, 190 (3d Cir. 2009) (internal citations omitted).

2. Urban Outfitters Plainly Violates A.R.S. § 44-1376.01

Plaintiff's allegations that Defendant spied on the time and place where she read emails sent to her violates the plain meaning of the statute.

"When interpreting state law, we follow a state's highest court; if that state's highest court has not provided guidance, we are charged with predicting how that court would resolve the issue." *In re Energy Future Holdings Corp.*, 842 F.3d 247, 253-54 (3d Cir. 2016) (quoting *Illinois Nat. Ins. Co. v. Wyndham Worldwide Operations, Inc.*, 653 F.3d 225, 231 (3d Cir. 2011)). In Arizona, courts "determine the plain meaning of the words the legislature chose to use, viewed in their broader statutory context." *See Columbus Life Ins. Co. v. Wilmington Tr., N.A.*, 255 Ariz. 382, 385 ¶ 11, 532 P.3d 757, 760 (2023). "Our task in statutory construction is to effectuate the text if it is clear and unambiguous. Absent ambiguity, we interpret statutes according to their plain language. When a statute's plain language is unambiguous in context, it is dispositive." *In re Drummond*, 2024 WL 740253, at *1 (Ariz. Feb. 23, 2024) (internal quotations omitted).

The statute here is unambiguous and Defendant does not argue that it is ambiguous. A.R.S. § 44-1376.01 prohibits the knowing procurement of a "communication service record" of any

Arizona resident "without the authorization of the customer." A.R.S. § 44-1376.01(A)(1). And the definition for "communication service record" is very broad:

> "Communication service record" ***includes*** subscriber information, ***including name***, billing or installation address, length of service, payment method, telephone number, ***electronic account identification*** and ***associated screen names***, toll bills or ***access logs***, ***records of the path of an electronic communication between the point of origin and the point of delivery*** and the nature of the communication service provided, such as caller identification, automatic number identification, voice mail, ***electronic mail***, paging or other service features.

A.R.S. § 44-1376(1) (emphasis added).

Read in the light most favorable to Plaintiff, Plaintiff properly alleges that Defendant procures her "subscriber information" in order to gain Plaintiff's "subscriber engagement data" and procure "directional insights" to Plaintiff "behaviors." Compl. ¶ 34. This would necessarily require Defendant to correlate Plaintiff's "behavior" with her "name" or "electronic account identification" or "associated screen name" that is traceable to her. *Id.* By collecting the time and place each email was opened, Defendant procured an "access log" of the time and place where the email was opened. Compl. ¶¶ 36-37. "Access log" is a computer science term used to describe a file "that records all events related to … user access to a resource on a computer." Arfan Sharif, *What Is An Access Log*, Crowdstrike (Dec. 21, 2022), https://www.crowdstrike.com/cybersecurity-101/observability/access-logs. An access log allows "software developers [and] operation engineers … to monitor how their application is performing, who is accessing it, and what's happening behind the scenes." *Id.* The information collected by an access log includes the date and time of client access, the client IP address or hostname, and username. *Id.* "An access log is a list of all requests for individual files—such as … embedded graphic images and other associated files that get transmitted—that people … have made from a website. … These server logs record the history of page requests made to the server and other pertinent information." Andrew Zola, *Access Log Definition*, TechTarget,

https://www.techtarget.com/searchsecurity/definition/access-log (last updated January 2022). This is exactly the kind of information that is captured by email spy pixel in order to learn "engagement data" and "directional insights." Compl. ¶¶ 28-38.

Defendant makes an astonishing argument that "electronic mail" does not mean email but gives no reason why except to say that "[w]ords in a statute, must be read in context." MTD at 12 (citation omitted). Of course, the plain meaning of "electronic mail" is email. *See E-Mail*, Black's Law Dictionary (11th ed. 2019) ("Also termed *electronic mail*.").

Defendant next makes a half-baked analogy to *In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262 (3d Cir. 2016) ("*In re Nickelodeon*"), to argue that a statute passed in 2007 is no longer applicable. MTD 12-14. That is ludicrous on many levels. First, the statute in *In re Nickelodeon*, the VPPA, is a completely different statute, and its substantive interpretation has no bearing on the instant case. Second, unlike *In re Nickelodeon* and the VPPA, the email technology here operates exactly the same as it did in than in 2007. Compl. ¶ 28 ("Not much has changed between 2008 and today."); *cf. In re Nickelodeon*, 827 F.3d at 288 ("We of course appreciate that the passage of time often requires courts to apply old laws in new circumstances.") (citations omitted). Third, even the court in *In re Nickelodeon* recognized that violations of the VPPA—a law passed in 1988—can occur through modern technology. *In re Nickelodeon*, 827 F.3d at 289 (emphasizing that there is no disagreement with the First Circuit's holding in *Yershov v. Gannett Satellite Info. Network, Inc.*, 820 F.3d 482 (1st Cir. 2016), where the court held that "GPS coordinates of the phone's location at the time the videos were watched" is sufficiently personally identifiable information); *see also Braun*, 2023 WL 7544160, at *3-4 (finding allegations of disclosure of plaintiff's "Facebook User ID" and video watching history sufficient to assert a VPPA claim).

Defendant also argues that the legislative history "clearly demonstrates that the Legislature was concerned with telecommunications carriers and records of subscribers of telecommunications services." MTD at 14; *see also id.* at 9-11 (discussing the legislative history). This argument is also unavailing. First, in Arizona courts do not rely on legislative history to derive when the plain meaning of the statute is unambiguous. *State v. Ewer*, 254 Ariz. 326, 331 (2023) ("We do not consider legislative history when the correct legal interpretation can be determined from the plain statutory text."). As described above, A.R.S. § 44-1376 is unambiguous. Second, contrary to Defendant's assertion, the legislative history shows that the A.R.S. § 44-1376.01 was passed to prevent the kinds of invasions of privacy that occurred during the Hewlett-Packard Pretexting Scandal which included email tracking with spy pixels. Compl. ¶¶ 14, 27; Arizona House Bill Summary, 2007 Reg. Sess. H.B. 2726 ("In January 2007, Congress passed the Telephone Records and Privacy Protection Act …. [the Arizona statute] prohibits a person from knowingly procuring … a communication service record."). Third, as Defendant noted, the statute was specifically amended—a year after it was originally passed—to include "communication service records," indicating that the statute is ***not*** limited to telephone pretexting. MTD at 10-11; Arizona House Bill Summary, 2007 Reg. Sess. H.B. 2726.

Put simply, the plain language of A.R.S. § 44-1376 prohibits the surreptitious collection of email records which includes the time and place where specific emails were read by Plaintiff.

IV. CONCLUSION

Plaintiff has properly alleged Defendant violates A.R.S. § 44-1376.01 by tracking her email activity, and this Court has subject matter jurisdiction to hear this claim given that Plaintiff has Article III standing for her claim. For all the foregoing reasons, the Court should deny Defendant's Motion to Dismiss in full.

Dated: March 22, 2024

Respectfully submitted,

KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT

/s/ Kenneth J. Grunfeld
Kenneth J. Grunfeld
PA Bar No.: 84121
65 Overhill Road
Bala Cynwyd, PA 19004
Tel: (954) 525-4100
grunfeld@kolawyers.com

Yitzchak Kopel*
BURSOR & FISHER, P.A.
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Tel: (646) 837-7150
Fax: (212) 989-9163
E-Mail: ykopel@bursor.com

*Pro Hac Vice Application Forthcoming

Attorneys for Plaintiff and the proposed class